Power Utility Automation Cybersecurity: IEC 61850 Specification of an Intrusion Detection Function

Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, Eric Savary

Power Utility Automation Cybersecurity: IEC 61850 Specification of an Intrusion Detection Function

M. Kabir-Querrec
Euro-System, F-38760 Varces, France
Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France

S. Mocanu & J.-M. Thiriet
Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France
CNRS, GIPSA-lab, F-38000 Grenoble, France

E. Savary
Euro-System, F-38760 Varces, France

ABSTRACT: The IEC 61850 standard defines a global framework for designing power utility automation systems. The main goal of IEC 61850 being interoperability, it brings information and tools for both system modelling and communication architecture. But cybersecurity measures and propositions are scarce. They should be a priority. To help fill this lack of cybersecurity, we specify a fully IEC 61850-compatible intrusion detection function. This paper explains the procedure of defining functions and necessary model objects consistent with the standard requirements. We then detail our intrusion detection function.

1 INTRODUCTION

1.1 *Context*

Information and Communication Technologies have been pervading monitoring and control systems for a few decades, especially in substations of the electric power transmission and distribution grid. They allow reading measurements remotely, retrieving logs and sending commands. Such communication was primarily characterized by proprietary protocols and closed networks, hence bringing security through obscurity and through isolation. Aspirations for vendor interoperability along with ever growing complexity of technologies led to standardization of networks and protocols used within substations, resulting particularly into the IEC 61850 standard - Communication networks and systems for power utility automation (TC57). This standard is key to substation automation systems (SAS) but seriously lacks digital security measures when substations are interconnected with more global and open networks, which makes them exposed to cyber incidents, whether intentional or not. Cyber vulnerabilities are threats to the safety of the SAS and thus to the safety and the reliability of the whole power grid.

1.2 *Scope of the paper*

The purpose of this paper is to propose a specification of a cybersecurity function compatible with the IEC 61850 standard, especially with the data object model it defines. This would allow for a future integration directly into Intelligent Electronic Devices (IEDs), as a function of its own along with other more common functions such as “distance protection” or “synchronized CB switching” (Circuit Breaker). Hence our cybersecurity function must be designed following the scheme given in the standard. All definitions and statements stipulated in the IEC 61850 standard make up an abstract model, meaning they are independent of any actual implementation or technology. And so is the specification of the cybersecurity function presented in this paper. It is about defining the objects and concepts that the standard lacks to address the problem of managing intrusion detection.

This paper is organized as follows: we first briefly explain the key concepts introduced by the IEC 61850 standard and relevant to this work. The next section is about IEC 61850 functions specification process. Section 3 is an overview of several papers related to the cybersecurity of substation automation system and the understanding and modelling of IEC 61850 concepts. The presentation of the proposed cybersecurity function comes in section 4. Conclusion and a discussion about possible further work end the paper.

2 IEC 61850 STANDARD

Our work must be considered in the scope of the international standard IEC 61850. Developing standard communication protocols for Substation Automation Systems (SAS) has long been considered essential by the whole power utility community. They would support interoperability, which is a common goal for electric utilities, equipment vendors and standardization bodies. As stated in the introductory part of the standard (IEC 61850 – 1), in-

teroperability is the ability for all the IEDs of a SAS "to operate on the same network or communication path sharing information and commands". From the user point of view interoperability also means interchangeability, that is replacing an IED by another one whoever the manufacturer is, without changing anything in the other elements in the system.

Another important objective of SAS standardization is to develop communication protocols able to support future evolution of technologies.

2.1 *Data Object Model*

One of the main contributions of the IEC 61850 standard is an object-based data model for functions and services, which brings functional decomposition and information modeling. The figure below illustrates this data object model. An application function is decomposed into the smallest entities called Logical Nodes (LN). LNs are characterized by their data and methods, and exchange data with each other.

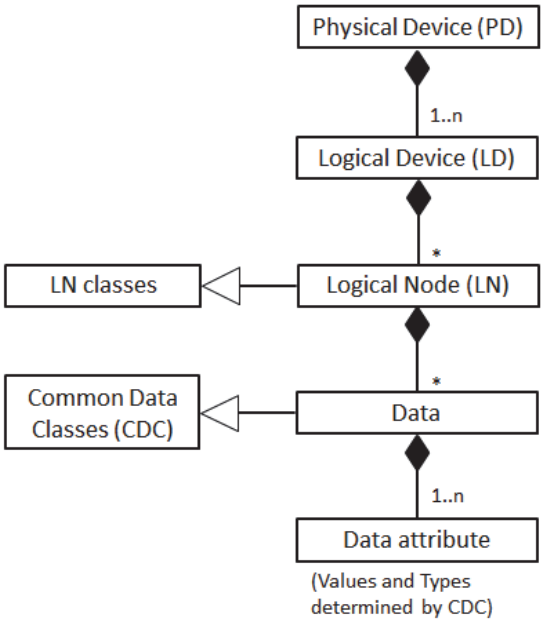

Figure 1. IEC 61850 Data Object Modeling

All the LNs required to complete a specific function are aggregated along with relevant data sets into a virtual device called Logical Device (LD). A real Physical Device (PD), such as an IED, can be composed of many LDs.

Logical nodes are organized in thirteen specific categories. The names of LNs are standardized as follows: Group designator / Three-letter abbreviation of function / Instance ID. For instance XCBR1 belongs to the "Switchgear" group and models a switch with circuit breaker capability, first instance (IEC 61850 – 7.4). Note that in this article we deliberately do not respect this standardized naming to keep new object names understandable and ensure that our function description is easy to follow. For instance CYAN will stand for "CYbersecurity ANalyzer" and CYComChkSingle for "CYbersecurity Communication Checker for a Single frame". The standard defines logical node classes regarding substation common functionalities, giving mandatory and optional LN information. Part 7.3 also provides Common Data Classes describing necessary data: name, type, trigger option, value range, etc…

2.2 *Information exchange*

In the context of the IEC 61850 series, only LNs exchange data and therefore a function exchanging data must be composed of at least one LN. Information exchange between two LNs is defined by the PICOM concept, Piece of Information for COMmunication. By definition, a PICOM is "a given data element or block of data on a given logical path with a given communication attributes" (Cigré 2001). To keep consistency with the data object model described above, PICOM can be spoken of as a class stipulating information transfer between a source LN and a sink LN. This class has many attributes characterizing either the information content (such as data type, name, value…) or the communication requirements (such as source and sink names, priority of transmission, data integrity…). Some of those attributes must be covered by any message when others are to be considered at configuration time or for data flow calculations. PICOMs are related to the application layer and do not represent the actual format and structure of the data over the physical network.

A device is fully described by its functions (LNs) and its transmissions (PICOMs). For unambiguous machine-to-machine communication, PICOM identifiers and attributes shall be understandable by every machine involved in the substation automation system. Hence defining new functions must comprise the task of PICOMs' specification along with the logical components (LNs and LDs). The standard defines message types based on a grouping of the performance related PICOM attributes:

- Type 1 – Fast messages,
- Type 2 – Medium speed messages,
- Type 3 – Low speed messages,
- Type 4 – Raw speed messages,
- Type 5 – File transfer functions,
- Type 6 – Time synchronization,
- Type 7 – Command messages with access control.

Choosing adequate message types will improve the whole SAS performance.

2.3 *Communication architecture*

Parts 7-2, 8-1 and 9-2 of the standard propose the communication architecture shown in Figure 2. This data flow method is another major contribution of this standard.

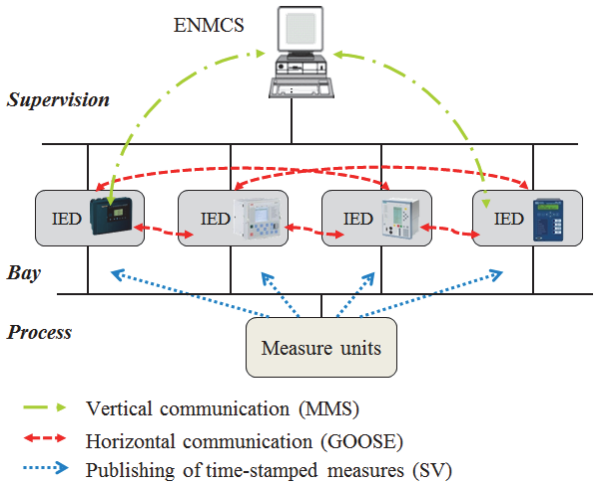

Figure 2. 61850 communication architecture (Nachar 2013)

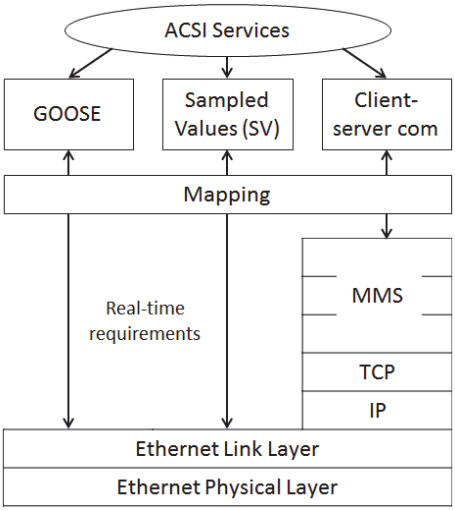

Figure 3. OSI mapping of IEC 61850 protocols.

At the supervision level, the Electrical Network Monitoring and Control System (ENMCS) is connected to the IEDs over the station bus that operates MMS (Manufacturing Message Specification). This protocol is based on the TCP/IP layers (Fig. 3) and allows traditional supervision operations: read, write and report. Horizontal communication between bay-level IEDs is allowed via GOOSE (Generic Object Oriented Substation Event) messages, directly mapped on the Ethernet data link layer to meet the time performance required for such data exchanges, that is 4ms end-to-end transfer time. Such messages work on a publisher/subscriber mechanism on broadcast MAC addresses. Sampled Values (SV) are used for transmitting digitized power quantities from process systems, mainly current and voltage values.

2.4 *Defining new functions*

The task of defining SAS functions and the data elements they make use of has to follow some rules to ensure the interoperability between all the components of the global system (Xu et al. 2007). It consists of three steps: describe the function and its decomposition into LNs, then describe each of the LN and the exchanged PICOMs, and finally detail the PICOMs. An IEC 61850 function is then defined by:

- Task description: a formal description of the function task and its context of execution,
- Starting criteria: the specific reason of the function initiation,
- Result or impact: the output of the function,
- Performance: total requested response time must be guaranteed, possible additional criteria may be accuracy of synchronization...,
- Function decomposition: decomposition into LNs,
- Interactions with other functions: data exchanged with other functions, will result in definition of PICOMs.

A similar scheme has to be followed for describing LNs:

- Introduction: task description and context of execution,
- Starting criteria,
- Input and output by PICOMs,
- Operation mode: safe behavior in case of degraded data exchange must be provided,
- Performance: based on performance attributes of PICOMs.

To fully specify a LN, this description is not enough. The LN data have to be explicitly defined, that means that the following questions have to be answered: Of which type is this data object? What are its data attributes? Of which type is each of those attributes? Etc… This is a stepwise process summarized in diagram in Figure 4. The idea is to use the data elements defined by the standard when appropriate and to enrich the model with new data elements required to fulfill the task of the function.

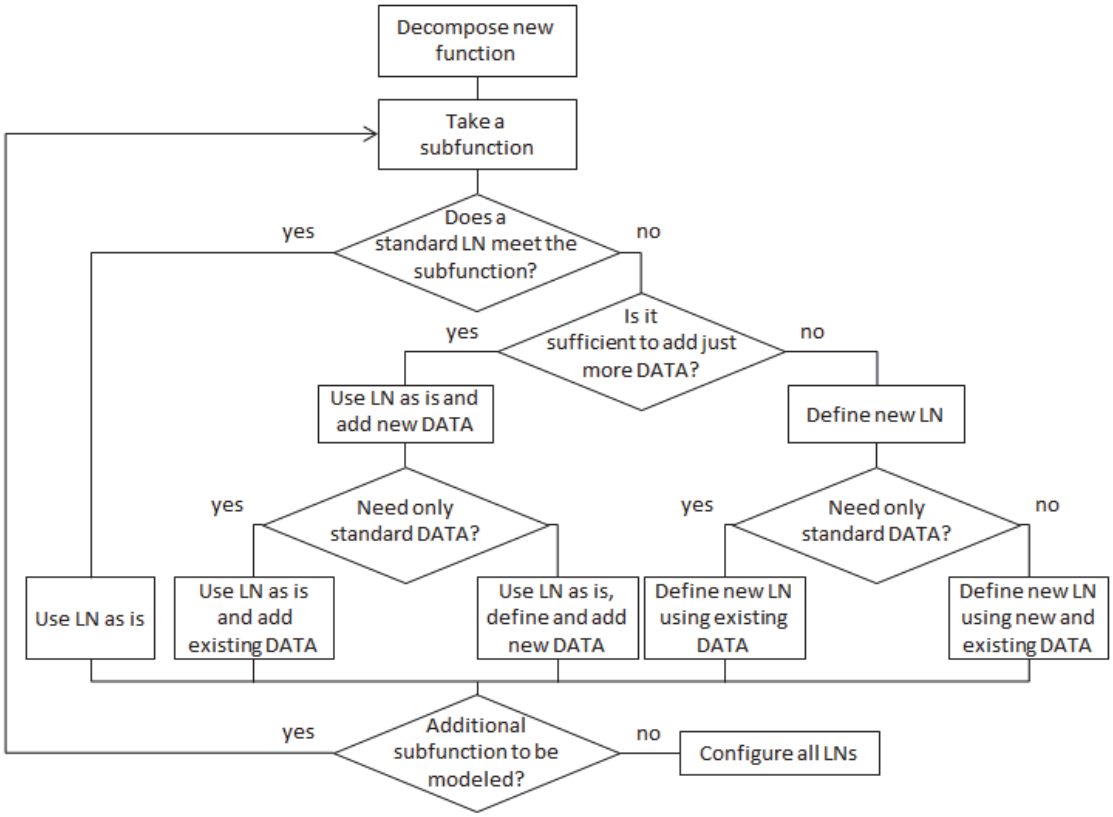

Figure 4. IEC 61850 function extension rules.

To build a new functionality, the first step is to decompose the function into subfunctions. If a LN of the standard meets the characteristics of the subfunction, use it as is. Otherwise, if adding existing or new data to an existing LN is not sufficient, then create a new LN. The same flow can be run to define all the data of a LN along with their existing and new data attributes.

Once the data model description has been completed, the logical connections still have to be written. They depict the information exchange between LNs and hence between functions. Then, the new functionality is fully specified. As mentioned earlier, PICOM description provides information about semantics, logical point-to-point connection, performance requirements and type of data.

3 CYBERSECURITY FOR SMART-GRIDS SUBSTATIONS

3.1 *Intrusion and anomaly detection*

The purpose of intrusion detection is to monitor a network or a system activity to detect attempts to gain unauthorized access or to cause damages. Intrusion detection systems (IDS) are either host-based or network-based. The first category is a software module running on a device of the network and analyzing incoming and outgoing packets. Network-based IDSs are independent devices placed at strategic points of the subnet. They perform analysis on the traffic to and from all agents of the network. IDSs and firewalls are not to be confused. While the latter limit access at the entry point of a network segment to prevent intrusion, IDSs check for an attack from inside it and generate alarms. There are two types of intrusion detection approaches:

- Signature-based: to detect known attacks only,
- Anomaly intrusion detection: to detect known and unknown attacks by quantifying how much the observed behavior deviates from normality.

The anomaly-based detection was first introduced in 1985 by Dorothy E. Denning. In (Denning 1987) she proposed an intrusion detection model based on the idea that security violations can be detected by monitoring system audit records for abnormal patterns of system usage. She described a complete model emphasizing the importance of the metric and statistical analysis applied to each particular activity profile. Her idea was to introduce a system-independent model in the context of computer sciences. Using such a model in the particular case of industrial applications with embedded systems would mean to define these attributes even more carefully in accordance with the context, especially metrics and statistical models.

3.2 *IDS dedicated to industrial control systems*

A possible way of implementing an anomaly detection system is by analyzing whether the system is in an acceptable or a critical state. This approach can

be correlated to Fault Detection research field where measurable variables are monitored to estimate if the system is approaching some critical state. Such works are presented in (Jin et al. 2006) and (Fovino et al. 2012), although the latter makes use of traffic analysis to update and forecast an image of the system.

A more common approach is communication-based IDS. It can be implemented by specifying normal behavior as a baseline and then checking whether the actual network traffic agrees with this baseline. Snort is an open-source software for IP networks which uses such rules. (Premaratne et al. 2010) presents an IDS dedicated to IEC 61850 automated substations, specifying Snort rules. But using only rule-based detection seems to mean designing either a very generic IDS which seems dangerous or an IDS totally dedicated to a single equipment of a defined infrastructure which is properly inconvenient in case of deployment.

As a countermeasure to the non-adaptivity of IDS to potential normal evolution of system usages, (Sekar et al. 2002) combines specification of rules with probabilistic techniques. The concept is very valuable but may be difficult to implement for embedded system networks with real-time constraints.

Combining the two methods is also the strategy adopted in (Cheung et al. 2007) which proposes a three-level IDS for SCADA networks. The rule approach is for checking protocol characteristics and network access patterns when the probabilistic one is concerned with service availability.

All the methods mentioned and others have in common to be hosted by dedicated equipment. As highlighted in (Premaratne et al. 2010) IEDs have very low computational power and are not able to carry out cybersecurity functions as efficiently as those developed more recently. The authors of (Premaratne et al. 2010) hence recommend implementing the IEC 61850 IDS they designed within the gateway or if not feasible to connect the IDS to a port mirror of the gateway to ensure effective monitoring of the whole incoming traffic. The "critical state-based filtering system" described in (Fovino et al. 2012) is a part of the firewall through which all command packets from SCADA flow to the slaves. In (Linda et al. 2011), the IDS is implemented into an embedded network security cyber sensor at the entry point of the process network whose security is to be monitored. However it is worth working on the idea of an IED-compatible anomaly detection function for future more capable gears because a host-based IDS has the advantage of operating independently even if other IEDs are corrupted.

From this perspective, we propose in this work to design an anomaly detection function specific to the IEC 61850 protocol stack and compliant with the standardized data object model. It would thus be able to operate independently as an autonomous device or would be embedded as a module in an IED.

3.3 *Anomaly detection for IEC 61850 SAS*

SAS specificities make necessary to think up dedicated intrusion detection methods:

- As stated above, unlike conventional computers IEDs are generally embedded systems hence having limited computational resources.
- Industrial applications often rely on real-time operations with highly constrained time-requirements, as emphasized in the 2011 Alstom Network Protection and Automation Guide (Alstom Grid 2011).
- SAS run dedicated communication protocols such as Modbus TCP/IP, DNP3 and IEC 61850 communication stack.
- Control of transport and distribution power grid provided by SAS relies on a fixed network topology and known mechanisms specific to the application domain. In particular communication mechanisms are well defined and highly constrained.

Advantages can be taken out of this knowledge to attain the objective of a tailored IDS. Some examples of such an approach can be found in literacy. In (Cheung et al. 2007), a thorough study of Modbus specifications leads to enunciation of system behavior rules. Similarly, the author of (Diallo & Feuillet 2014) describes a Suricata-based IDS for Modbus industrial processes. The network-based anomaly detection system for substation automation presented in (Hong et al. 2014) identifies malicious multicast messages matching rules for known attacks. These rules were defined based on the GOOSE and SV specifications, given by the IEC 61850 standard. The choice of a network-based anomaly detection system seems relevant to deal with multicast packets. The device would just need to subscribe to all GOOSE and SV messages to parse them.

4 AN IEC 61850 CYBERSECURITY FUNCTION

4.1 *Scope*

A "System security management" function can be found in the standard. It allows the control and supervision of the security of the system against unauthorized access and loss of activity. It monitors and provides all activities regarding security violations. The core element of this function is the logical node named Generic Security Application (GSAL) whose role is to monitor violations regarding authorization, access control, service privileges and inactive associations. These two elements seem focused on authentication and privileges which is out of our scope. For this reason and also to keep things simple, we

chose to make our anomaly detection function an independent one for now.

The objective here is not to propose a classical IDS adapted for use in a SAS but to specify an anomaly detection function based on IEC 61850 stipulations, that is detecting incoherencies regarding the standard. To do so, all the specificities of IEC 61850 SAS have to be taken into account and IEC 61850 function definition rules have to be diligently followed.

The presented intrusion detection function task is quite traditional but must be expressed according to the IEC 61850. Figure 5 shows a model of an IDS implemented as a dedicated 61850 IED in a SAS. LNs of the model are correlated to corresponding IDS modules.

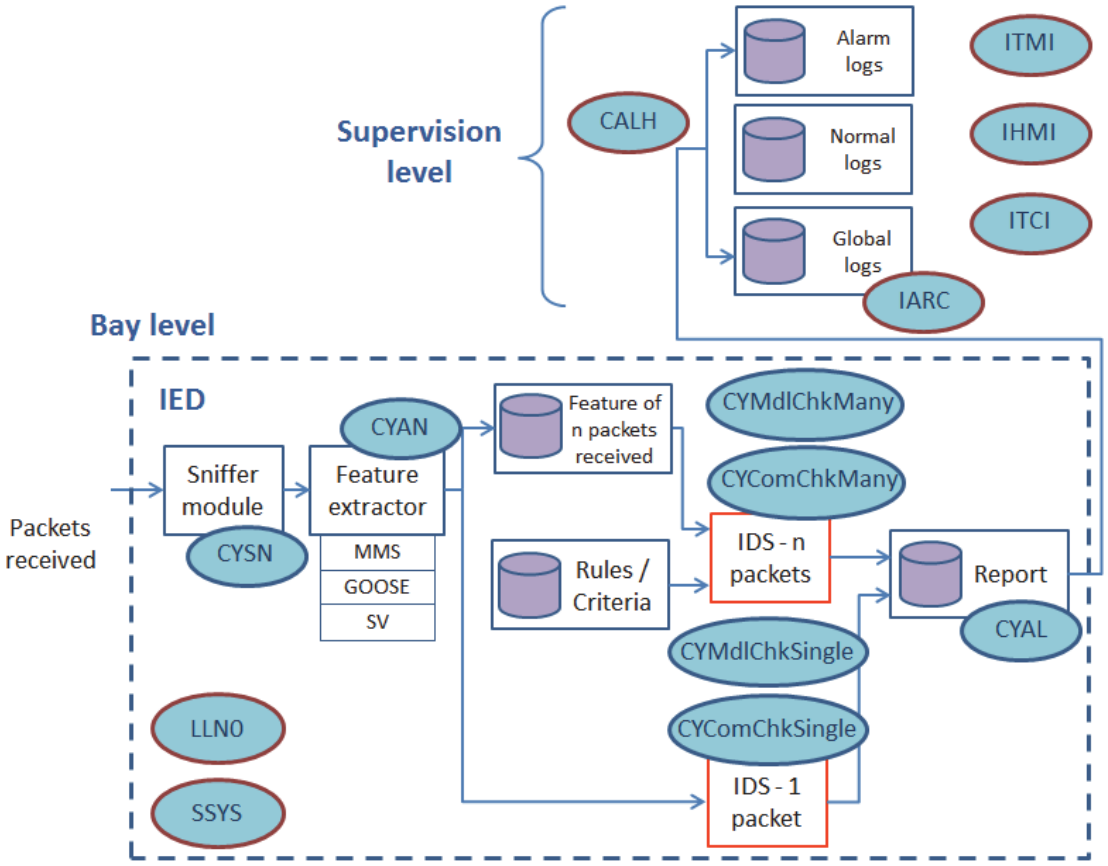

Figure 5. Model of an intrusion/anomaly detection function as a dedicated IED.

Following the function definition procedure given by the standard that we detailed earlier, this "Anomaly detection" function can be described as follows:

- Task: The anomaly detection function allows detecting anomalies in the system behavior. It analyzes input frames for feature extraction to check them for compliance with the communication model (syntax and semantics, and exchanges) and the system model. Results of this analysis are recorded and alarms are generated in case of deviance from the normality.
- Starting criteria: Reception of a frame.
- Result or impact: Results of the analysis are stored in logs and alarms are generated if need be.
- Performance: Total processing time (starting time + internal process time + overall transfer time per PICOM + delay time) and hence percentage of analyzed packets according to the throughput. PICOMs of type 2 and 3 would fit alarm generating and analysis report transmission. Also memory allocation should be well supported by the processor.
- Function decomposition: As given in Figure 6.
- Interactions with other functions: Network management, Event management, Alarm management, Archiving, System security management, Access security management…

4.2 *Function decomposition*

Our anomaly detection function is built from many cybersecurity-dedicated LNs we define below. These new LNs names start with "CY". Let us focus on GOOSE messages to describe the anomaly detection processing regarding communication only. We won't describe checker module dedicated to the application model, in grey in Figure 6 diagram. The approach regarding SV and MMS would be similar.

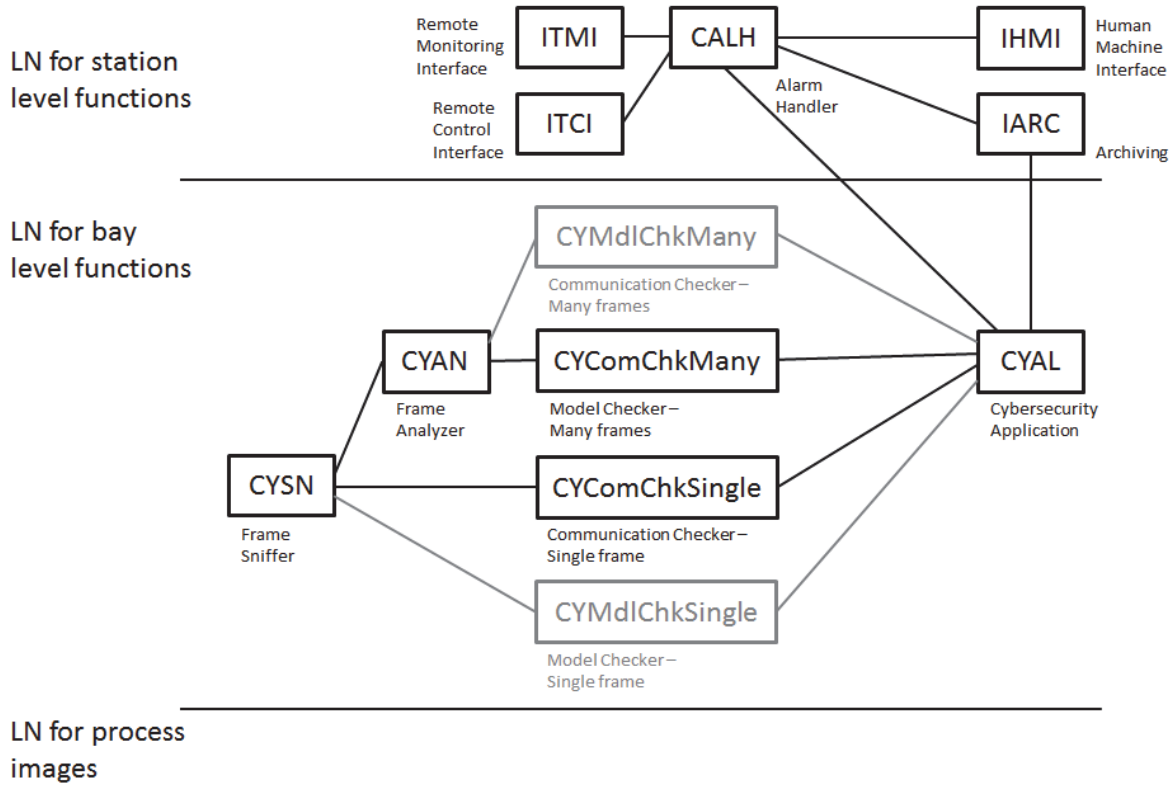

Figure 6. Decomposition of the anomaly detection function into interacting LNs on different levels.

For each new message, the sniffer (CYSN) gets the frame content and its reception time. There shall be an instance of CYSN per GOOSE type passing through the network under consideration and identified by the attribute GoID (GOOSE Identifier). When a data value changes in a message occurrence compared to the previous one, PICOMs are sent to the corresponding instance of CYAN whose role is to store and compute relevant features for each GoID. Reception times are also transmitted by PICOMs from CYSN to CYAN for every received message. Communication is then checked by two dedicated LNs: CYComChkSingle which verifies structure and communication parameters of a single frame, and CYComChkMany which checks consistency of messages received during a certain time slot. Useful information is carried by PICOMs from CYSN to CYComChkSingle and from CYAN to CYComChkMany. Analysis results are transferred to the supervision level through the CYAL node which is in charge with alarms and logs management.

LNs of the station level (Fig. 6) are classical IEC 61850 LNs.

4.3 *New data elements: excerpt*

Following the flowchart of Figure 4, we have fully specified our anomaly detection function covering all the data layers from LNs to basic types. While the purpose of this article is not to describe this function in detail, let us depict the bay-level LNs involved in the processing of a single frame: CYSN, CYComChkSingle and CYAL.

As shown in Table 1, CYSN mainly consists of the data object RecInfo of type Message Information (MSG). There was no existing LN for sniffing so we created CYSN. Note that CYSN input is not a PICOM as normally expressed for LNs but it pulls all incoming messages out of the reception buffer. The way it is done is a local issue, out of the scope of the IEC 61850 standard.

MSG is a new data class we made up for our purpose. Its main data attributes are GoFr (GooseFrame - a packed list of the frame items), recT (receptionTime - TimeStamp) and lgth (frame length - INT). The GoFr attribute of type “Packed List” is new. The “Packed List” type is defined by the standard as an “ordered list of types. Defined where the type is used.”

The specifications of logical nodes are given in the IEC 61850 standard as tables comparable to Table 1. All LN instances have a common structure with Common Logical Node Information, mandatory whatever LN it is, the following categories of data existing when relevant: Control Information, Status Information, Settings Information, Configuration-Description-Extension Information. Specifications of other objects of the model are given following similar templates. Hence specifying our cybersecurity function has resulted in such tables.

CYComChkSingle status information related attributes are of security violation counting common data class (SEC): PktStructDflt (Packet structure default), NumDataDflt (Number of data items wrong), AddrDflt (Source or destination address wrong), SqNumDflt (Inconsistency in sequence number incrementation), StNumDflt (Inconsistency in sequence number incrementation).

As an example of information exchange, here are the PICOMs transmitted by source LN CYAL, we can consider:

- Events to sink LNs CALH, IHMI, ITCI, ITMI.
- Diagnostic data to sink LNs IHMI, ITCI, ITMI. For sake of clarity these PICOM connections do not appear in Figure 6.

Table 1. LN class: Sniffer of LN group CY (Cybersecurity). Name: CYSN.

CYSN (Sniffer)			
Data Attr. Name	Attribute Type	Explanation	M/O
Common Logical Node Information			
		LN shall inherit all Mandatory Data from Common LN Class	M
Status Information			
RecInfo	MSG (Message Information)	Reception Information: Information about message reception	M

5 CONCLUSION AND FURTHER WORK

As an answer to the serious lack of cybersecurity considerations which IEC 61850 standard suffers from, this article presented an anomaly detection function. It has been designed by strictly following extension rules from the standard, thus ensuring consistency with the IEC 61850 model to not compromise the interoperability it aims to bring. LNs, DATA, attribute types, etc… were created to enrich the model with the necessary model objects.

Next step of our work is naturally implementing our function and test it. For these practical tasks, our laboratory is equipped with a platform dedicated to cybersecurity and interoperability of industrial control systems. Devices running on this test bench comprise IEDs (IEC 61850 but not only), PLCs, HMIs, supervision softwares and embedded boards for prototyping. It would also be interesting to realize the same work of specification and then implementation of other cybersecurity functions such as mapping of the communication architecture, resource availability, encryption, etc…

6 REFERENCES

Alstom Grid 2011. Network Protection and Automation Guide – New edition, Protective Relays, Measurement and Control.

Cheung S., Dutertre B., Fong M., Lindqvist U., Skinner K., Valdes A. 2007. Using model-based intrusion detection for SCADA networks. *SCADA Security, Proc. intern. scientific symp., Miami Beach, Florida, USA, 24-25 January 2007.*

Cigré 2001. REF. 180 2001 SC 34 WG 34.03 Communication requirements of data flow within substations

Denning D. E. 1987. An Intrusion-detection model. *IEEE Transactions on Software Engineering* SE-13(2): 222–232.

Diallo D., Feuillet M. 2014. Détection d'intrusion dans les systèmes industriels: Suricata et le cas de Modbus. *C&ESAR ; Proc. conf., Rennes, France, 24-26 November 2014*.

Fovino I. N, Coletta A., Carcano A., Masera M. 2012. Critical State-Based Filtering System for Securing SCADA Network Protocols. *IEEE Transactions on Industrial Electronics* 59(10): 3943-3950.

IEC TC57, IEC 61850 – Communication networks and systems for power utility automation (previously: Communication networks and systems in substations).

Jin X., Bigham J., Rodaway J., Gamez D., Phillips C. 2006. Anomaly detection in electricity cyber infrastructures. *Complex Networks and Infrastructure Protection ; Proc. international workshop, Rome, 28-29 March 2006.*

Hong J., Liu C.-C., Govindarasu M. 2014. Integrated Anomaly Detection for Cyber Security of the Substations. *IEEE Transactions on Smart Grid* 5(4): 1643,1653

Linda O., Vollmer T., Wright J., Manic M. 2011. Fuzzy logic based anomaly detection for embedded network security cyber sensor. *IEEE Symposium Series on Computational Intelligence ; Proc., Paris, 11-15 April 2011*: 202–209.

Nachar, M. 2013. Technical report, Euro-System.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., Jian-Cheng Tan 2008. Evidence Theory based Decision Fusion for Masquerade Detection in IEC61850 Automated Substations. *Information and Automation for Sustainability, ICIAFS 2008; Proc. intern. conf., Sri Lanka, 12-14 December 2008*: 194-199.

Premaratne U., Samarabandu J., Sidhu T., Beresh R., Tan J.-C. 2010. An intrusion detection system for IEC 61850 automated substations, *IEEE Transactions on Power Delivery* 25: 2376–2383.

Sekar R., Gupta A. K., Frullo J., Shanbhag T., Tiwari A., Yang H., Zhou S. 2002. Specification-based anomaly detection: A new approach for detecting network intrusions. In ACM Press (ed.), *Computer and Communications Security ; Proc. of the 9th ACM Conference, Washington, DC, USA 18-22 November 2002.*

Xu, T., Hui Hou, Hongwei Yu, Dahai You, Xianggen Yin, Yangguang Wang 2007. Analysis on IEC 61850 Interoperability Support. *IEEE Power Engineering Society General Meeting:* 24-28.